JOURNAL OF INTERNET LAW

VOLUME 9
NUMBER 8

FEBRUARY 2006

EDITED BY DLA PIPER RUDNICK GRAY CARY

The NSA's Interception of Emails and Phone Calls in the US Is Unlawful

By Randy Gainer

The December 2005 disclosure by the New York Times that the National Security Agency (NSA) is intercepting email messages and telephone calls between persons in the United States and suspected members or affiliates of Al Qaeda outside the United States caused several Senators and others to question whether the NSA program is lawful. President Bush has repeatedly claimed that the NSA program is both constitutional and authorized by congressional action. This article discusses the publicly disclosed aspects of the NSA program and concludes that the NSA violates US law when it intercepts the email messages and telephone calls without a Foreign Intelligence Surveillance Court (FISA) court order.

THE NSA'S EFFORTS TO IDENTIFY AND MONITOR COMMUNICATIONS WITH AL QAEDA SUSPECTS

The NSA's "special collection program" began shortly after the September 11 attacks.[1] It was intended to monitor communications between Al Qaeda suspects located in Afghanistan and other foreign countries and members in the United States who may disclose threats to the United States. President Bush signed executive orders that permitted the NSA to monitor the communications without obtaining warrants from the Foreign Intelligence Surveillance Court[2] if the communication originated or terminated in a country other than the United States.[3] Officials familiar with the program told the *Times* that the NSA monitors about 500 Americans and others in the United States at a time under the program and has probably monitored several thousand during the four years the program has been in operation.[4] The administration continues to seek warrants from the FISA court if it wants to monitor a telephone call or email message *that begins and ends* in the United States.[5]

President Bush confirmed on December 17, 2005, that he had authorized the NSA program shortly after the September 11 attacks and has reauthorized it more than 30 times after reviewing the program about every 45 days. He termed the program "crucial to our national security" and said it was necessary due to "the threat of catastrophic damage to our homeland."[6]

President Bush, Attorney General Alberto Gonzales, and former NSA Director General Michael V. Hayden defended the NSA program at a December 19 news

Continued on page 10

IN THIS ISSUE

Randy Gainer is a partner in the Seattle office of Davis Wright Tremaine LLP. His practice emphasizes litigating computer system disputes and advising businesses about data security and privacy issues. See http://www.dwt.com/lawdir/attorneys/GainerRandy.cfm. The views expressed in this article are those of the author and not of Davis Wright Tremaine or any of its clients. This article is not legal advice and should not be used as a substitute for legal advice. © 2006 Randy Gainer. All rights reserved. The author thanks Kaustuv M. Das, an associate in Davis Wright Tremaine's Seattle office, for his assistance.

ASPEN
PUBLISHERS

JOURNAL OF INTERNET LAW

JOURNAL OF INTERNET LAW (ISSN# 1094-2904) is published monthly by Aspen Publishers, 111 Eighth Avenue, New York, NY 10011. Telephone: 212-771-0600. One year subscription (12 issues) price: $380. Single issue price: $36. To subscribe, call 1-800-638-8437. For customer service, call 1-800-562-1973. For article reprints and reprint quotes, contact *FosteReprints* at 1-866-879-9144. Postmaster: Send address changes to JOURNAL OF INTERNET LAW, Aspen Publishers, 7201 McKinney Circle, Frederick, MD 21704.

This publication is designed to provide accurate and authoritative information in regard to the subject matter covered. It is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional services. If legal advice or other professional assistance is required, the services of a competent professional person should be sought. —From a *Declaration of Principles* jointly adopted by a Committee of the American Bar Association and a Committee of Publishers and Associations.

The opinions expressed are for the purpose of fostering productive discussions of legal issues. In no event may these opinions be attributed to the authors' firms or clients or to DLA Piper Rudnick, Gray Cary or its attorneys or clients.

ASPEN
PUBLISHERS

Proving Web History: How to Use the Internet Archives

By Beryl A. Howell

Showing what content a Web site previously contained (as opposed to what is currently on the site) may help answer questions that attorneys confront in a myriad of cases, ranging from copyright and trademark infringement to business torts and defamation. Showing that a particular Web site is currently using copyrighted text or images or protected marks may be all that is needed in a case, but documenting prior versions of the Web site can be critical to establish the scope or extent of the illegal or tortious conduct, the amount of the damages, or the requisite mens rea.[1] When the Web site at issue or the offending content on it has been removed or modified, the most effective, if not the only, way to document the content is to review prior versions stored in online archives of Internet sites.

Specifically, in trade secret and misappropriation cases, showing that the same information claimed to be secret or confidential has previously been made publicly available by the claimant, such as on the claimant's Web site, can be probative if not case dispositive. Diligently searching archived versions of the claimant's Web site for such evidence can be worthwhile.

Similarly, capturing evidence from archived Web sites is helpful in intellectual property infringement cases as well. For example, in cybersquatting and typo-squatting cases, where a trademarked name or a slightly misspelled trademarked name (*e.g.*, *mcrosoft.com*) has been registered as a domain name and used as an online address for a Web site, evidence from archived versions of the Web site may establish the period of time the offending Web site has been operational and the types of goods or services offered on the site over time. This evidence can help establish intent and harm. In cyberstuffing cases, where popular trademarked names are repeatedly embedded in hidden metatags and transparent text on a Web site, search engines will pick up on the trademarked names and push the infringer's Web page to the top of search engine results, diverting business from the trademark owner's site. Even if the Web site is modified after the infringer is notified of the claim, documenting the cyberstuffing activity on archived versions of the Web site can establish the nature of the offending activity, its scope, and duration.

No matter the legal context, gathering evidence of prior versions of Web sites should be performed in a careful forensic manner with cognizance of the underlying technology used in the archiving process. This article will review strategies and methods for capturing prior versions of Web sites from the most popular of the archives and considerations that counsel should be prepared to address in authenticating this evidence.

"MAP" OF ARCHIVES

At the outset, archived versions of Web sites are available for free at multiple sites. The federal government, in particular, archives government Web sites and makes those archives accessible online. For example, the US Government Printing Office, in partnership with the University of North Texas, provides online access to federal Web sites that have ceased operation on a site called the CyberCemetery.[2] The archived deceased Web sites include Access America, Advisory Commission on Intergovernmental Relations, Office of Technology Assessment, and others. Similarly, the Electronic Research Collection (ERC),[3] which is a partnership between the United States Department of State and the Federal Depository Library at the Richard J. Daley Library, University of Illinois at Chicago (UIC), makes available the US Department of State Web pages archived from 1998 through January 2001. In addition, the National Archives and Records Administration harvested all of the federal agency public Web sites as they existed at the end of the presidential term on January 20, 2005, and makes these archives available at the 2004 Presidential Term Web Harvest site.[4]

Archives of Web sites that are not associated with the federal government are available at several sites. The Library of Congress sponsors a project called Minerva (Mapping the INternet Electronic Resources Virtual Archive), which harvests Web sites based on subject matter and then provides the collections as an archive, rather than try to harvest every Web site. The collections currently available include: Election 2002 Web Archive

Beryl Howell is a Partner and heads the Washington, DC, office of Stroz Friedberg, LLC, a computer forensics and electronic discovery consulting and technical services firm with offices also in New York City, Minneapolis, and Los Angeles. She formerly served as a New York federal prosecutor and General Counsel of the US Senate Committee on the Judiciary. Research assistance for this article was provided by Donald Allison and Jessica Reust, computer forensic examiners, and George McLean, Evidence Technician at Stroz Friedberg, LLC.

(July 1, 2002 - Nov 30, 2002);[5] September 11, 2001 (September 11, 2001 - December 1, 2001);[6] and Election 2000 (August 1, 2000 - January 21, 2001).[7]

Certain Internet search engines, such as Google and Yahoo, also make archived Web sites available. The Google archive provides access to the last cached version of a Web site, but not to prior versions. These cached Web sites are a backup in case the original page is unavailable and are useful since they show the date and time stamps for when each page on the site was retrieved by Google. Google and other search engines often index a Web site about once a month, but Google explains that the "cache is the snapshot that we took of the page as we crawled the web" and cautions that "[t]he page may have changed since that time" or "[t]his cached page may reference images which are no longer available." Google states that many factors affect how often it indexes a site, but a 2003 survey showed that Google revisited most sites within one month.[8] Therefore, unless a page is defunct, a Google cached site often will be 30 days old or less. To look farther back in time, the Internet Archive is probably a better bet. Sites may not be cached if they have not been indexed or if the owners have requested that the content not be cached. The date-time stamps on the Google archive may be helpful in establishing, for example, when a site stopped operating within the last six months. If a site is no longer available online, a visit to the Google cache may indicate the date when the site was last indexed.

Yahoo has recently added the ability to view cached pages by clicking on a link entitled "cached." As with Google, clicking on "cached" brings up a copy of the Web page as it appeared when it was last crawled by the search engine. By contrast to the Google cached sites, however, the Yahoo archive does not date-stamp the version of the cached site but simply notes the following: "It's a snapshot of the page taken as our search engine crawled the Web. The Web site itself may have changed." To check the previous versions of the Web site, Yahoo directs users to the Internet Archive. As discussed in more detail below, the Internet Archive contains the most extensive archive of Web sites in terms of period covered, number of Web sites and pages archived, and the number of prior versions of Web sites archived.

Other search engines that provide cached Web sites include *search.msn.com* (MSN), *ask.com* and *teoma.com* (both from Ask Jeeves), *clusty.com* (from meta-search engine Vivisimo), and *Gigablast.com*. Of these, Gigablast may be the most helpful in researching historic Web sites because its search engine results include the date that the Web page was last modified, as well as the date that the page was last indexed by Gigablast. Gigablast also provide links to the cached site, a stripped version of the site without graphics, and a link to "older copies" found on *archive.org*.

THE INTERNET ARCHIVE AND THE WAYBACK MACHINE

The Internet Archive[9] is a free online resource that was created in 1996 to build a digital library of Web pages and other cultural artifacts in digital form with the purpose of offering permanent and free access to researchers, historians, scholars, and the general public.[10] Internet Archive provides not only an archive of websites but also of open source movies, feature films, cartoons, historic newsreels, and news video and music.

Five years after its creation, in October, 2001, the Internet Archive launched the Wayback Machine, which provides the public with a free online service to search for and access archived Web sites. The name of the search service is derived from the Rocky and Bullwinkle cartoon in which the characters of a bow-tied dog, Mr. Peabody, and his boy assistant, Sherman, used a time machine called the WABAC Machine to travel back in time to famous events in history.

The Web pages are collected for the Internet Archive using a search engine technology called Alexa Crawl that traverses the Internet taking snapshots of Web sites. The Alexa Crawl currently captures about 1.6 terabytes (1600 gigabytes) of Web content per day and takes about two months to complete a snapshot of the more than 16 million Web sites accessible online.[11] This search-and-copy engine is owned and operated by Alexa Internet, a for-profit company that offers a free toolbar and a number of statistical services to subscribers based upon the Web content and usage information collected. The company donates a copy of each crawl of the Web to the Internet Archive, which may make the crawl results available after six months. Thus, there is a six- to 12-month lag between the date that a site is crawled and when it appears for free use in the archives of the Wayback Machine.[12] Alexa Internet is now offering a fee-based service to access its crawl results data before it goes to the Internet Archive.[13]

The Alexa Crawl does not purport to capture all Web sites accessible on the Internet, but instead prioritizes the Web sites and pages to copy based on the number of times that a Web site is requested through the Alexa search engine. Thus, not every Web site has an equal chance of being copied or copied in full. Alexa Internet uses a rating system for content that will be captured. Content that is not popular may be deliberately omitted if not visited often. This is related to Alexa's business model for selling databases of frequently visited sites to customers. The result is that the Wayback Machine does not hold archived versions of all Web sites of copies of every page for the Web sites that are archived.

In addition, sites may not be archived if they are password-protected, the site owners have requested exclusion from the Wayback Machine, or the crawler is blocked by use of a technical flag installed by the site owner called robots.txt, or the site is otherwise inaccessible. When the site is blocked by request or use of a robots.txt flag, the Wayback Machine search engine will indicate this with an error message, such as "blocked site error" or "robots.txt query exclusion error."

At the inception of the Wayback Machine, the Internet Archive contained 100 terabytes of data that was growing at a rate of 10 terabytes per month. By 2005, the amount of data stored in it is more than a petabyte, with a growth rate of 20 terabytes per month, making the Internet Archive the largest data archive in the world. All of this data is stored in huge server farms in the Presidio of San Francisco.

The archived Web sites are stored across multiple servers. A version of a particular Web site that is shown as indexed on the Wayback Machine may not be available at the time when a user wants to access it. A replica of the Internet Archive is stored at the Bibliotheca Alexandrina in Egypt.[14] If a version of a particular Web site cannot be accessed on the Internet Archives' primary site, the replica site can be checked.

The replica on the Bibliotheca Alexandrina Web site is not updated frequently or recently, however, and it does not contain as much content. Test searches conducted on *archive.org* reveals many Web sites that do not appear on Alexandrina's Web site. For example, a search for *cnn.com* yields results for pages from July 2000-September 18, 2001, on the Alexandrina's Web site, while the *archive.org* site has version from November 26, 2004.

To use the Wayback Machine, users simply go to the *archive.org* Web site, and type in the Internet address[15] in the provided search box. Any versions of the Web site corresponding to the Internet address that are archived on the servers of the Internet Archive will pop up in a chronological list. A user can review this list and select the version or date for review by clicking on the selected date. The archived version of the Web site for the date selected will then appear and can be reviewed.

The nature of the legal dispute may require analysis of multiple archived versions of a particular Web site in order to establish whether and how content changed. For example, in a contract dispute, the question of whether a party offered services or items in violation of terms in the license at issue may require documenting changes in a party's advertised offerings on its Web site during and after expiration of the license term. Critical text may simply be eyeballed as part of this analysis to document changes over time. In addition, the Wayback Machine notes changes in an archived Web site with an asterisk. This asterisk system alerts only to changes in text or graphics and not to modifications in internal or external links and or in the source code for the Web site. This may become critical if, for example, the archived Web site is cited as evidence that it was used to link to an offending site. The link to the offending site in the archive version may not, in fact, have existed or existed in the same form at the time that version of the Web site was copied for the archive.

The Wayback Machine also offers a free service of comparing any two versions of an archived site using a technology called DocuComp, which is a patented algorithm licensed by Advanced Software for use in the Wayback Machine. The comparison can show how the contents, including text, images, and links, have changed over time and between any two versions being compared.

"MISSING" ARCHIVED WEBSITES

When a search for an archived Web site has negative results, this does not mean that the Web site does not exist, is not archived, or is only of current vintage. The Web site may have been excluded from the archiving process or in fact, the Web site may be archived but review of the archived versions is blocked. The Internet Archive takes steps to avoid archiving web sites for which the owner has indicated a preference to be excluded. A universal technical standard that indicates an exclusion preference is called the standard for robot exclusion (SRE). A file called robots.txt can be added to the header information on a Web site or specific Web page by an owner, and a denial or disallow command within that file can serve as a flag that the owner does not want the entire Web site or particular Web pages copied or scanned by a Web crawler. In other words, the directions in the robots.txt file can be set to allow full or partial copying or copying exclusion. The Alexa crawler respects this preference and will not copy those sites or pages with a robots.txt file embedded.[16] Alexa Internet and Internet Archive take this respectful technology a step further: When robots.txt is added to a Web site, Alexa will exclude the site from being copied by its crawler, and the Internet Archive will go back into archived sites to remove content already captured.[17]

In addition, intellectual property owners who believe that infringing activity is occurring on a Web site may contact the Internet Archive and request exclusion of the offending Web site. The Internet Archive provides specific directions to copyright and trademark owners seeking to have third-party Web sites containing infringing works removed from the archive. These owners must specifically identify the work allegedly being infringed and where it is located within the Internet Archive collections, contact information, and a statement made under penalty of perjury that use of the work is unauthorized by the copyright owner, along with an electronic or physical signature.[18]

The Internet Archives' respect for the exclusion preference of Web site owners and compliance with its own stated policy to remove Web sites with robots.txt flags is the subject of a recent suit in the Eastern District of Pennsylvania brought by Healthcare Advocates against the Internet Archive for, *inter alia*, breach of contract and misrepresentation due to a failure to block access to the plaintiff's archived Web sites.[19] The plaintiff operates a Web site that describes the services of the company, including helping the public get reimbursements for health care expenses, reporting on medical research, providing doctor referrals and information on discount prescriptions and healthcare plans. The company claims copyright in all of the Web site content. In mid-2003, the plaintiff installed the denial text string in the robots.txt file on the computer server hosting its Web site with the expectation that the Internet Archive would prevent users of the Wayback Machine from gaining access to the archived versions of its Web site.

Nevertheless, in another case brought by Healthcare Advocates against a competitor for misuse of proprietary and trade secret information, the defendant's counsel was able to access the archived versions of the plaintiff's Web site on the Wayback Machine by successfully circumventing the security offered by the denial text string in the robots.txt file. This circumvention was apparently facilitated by the fact that "the mechanism preventing www.archive.org from searching a particular web site's host computer server for a denial text string in the robots.txt file more than once per day was 'broken.'" In other words, when the Wayback Machine receives a query for an archived version of a Web site, the Web site is pinged for the presence of a robots.txt file denial string. If the string is found, the query is blocked, but apparently persistent queries will overcome the block. The defendant's counsel in the underlying lawsuit conceded that the plaintiff's archived Web sites on the Wayback Machine had been searched and accessed in connection with that underlying case. That counsel is now co-defendants with the Internet Archive in Healthcare Advocates' suit for copyright infringement and computer hacking.

This lawsuit will test the scope and merits not only of the claims at issue but also the indemnification provision of the Internet Archive's terms of use. Specifically, the terms governing the use of the collection of archived Web pages is predicated on the user's agreement "to indemnify and hold harmless the Internet Archive and its parents, subsidiaries, affiliates, agents, officers, directors, and employees from and against any and all liability, loss, claims, damages, costs, and/or actions (including attorneys' fees) arising from your use of the Archive's services, the site, or the Collections."[20]

CAPTURING ARCHIVED WEB SITES

Once an archived Web site has been located, the methods of capturing the virtual pages in a concrete form for use in court can vary. One method is to print each page that appears on the computer screen. The person performing or supervising the search and printing can attest to the date, time, and process used to obtain the printout. This method shows static pages of the Web site without any of the links that may remain active, other than any advertisements pushed to the site, even in the archived state. Similarly, screen-shots of each page viewed can be saved electronically for incorporation into expert reports or affidavits.

Importantly, Internet browsers and specialized tools used by computer forensic experts for downloading Web sites with metadata intact can be used to capture not only the graphical display of a Web page but also the underlying html code that is driving the display. Simply using the file save function on a browser can preserve code that may reveal who authored a contentious Web page. Saving underlying code in the same way may reveal a trademarked name written over and over again in white-on-white text, indicating that it was meant to be revealed to crawling search engines but hidden from a consumer's (or competitor's) naked eye. If two or more archived pages are linked to each other, download tools can provide a fuller layout of a Web site with its underlying code. At trial, this fuller layout can be presented to the judge or jury, and links and related pages can be navigated, much as an historic user might have surfed them.

In addition, specialized software tools are available that allow dynamic presentations, including demonstrations of any link that remains active on the Web site. One such software tool, called Camtasia, can be installed on the computer used to access the archived site to record every keystroke and screen shot appearing during review of the cached Web site. The recording of the review session is documented real time in video-like form that may be stored on a CDR or DVD for submission to court. For example, in a business diversion case, a recording of the cached version of the defendant's prior Web site may be able to show links that remain active and purportedly direct potential customers to the plaintiff's products, but the links instead actually channel users to the defendant's sites.

Beware when capturing an archived Web site that different browsers display Web sites with differing degrees of accuracy and completeness, and this holds true for archived Web sites and Web pages as well. There are a number of different reasons why some Web pages look different depending on which browser is used to view the page, including browser adherence to Web page standards, browser support of different technologies, and Web sites that do not use Web page standard code. The World Wide Web Consortium (WC3) develops the standard elements for Web site programming, which some browsers adhere to and some do not. For example Firefox and Mozilla adhere to the WC3 standards, while Internet Explorer supports additional non-standard Web-programming technologies. The resulting difference in the way that Web pages are displayed may be as minimal as the color of the scrollbar to as inconvenient as the navigation menus not working or the site content not being displayed at all.

A Web site that uses or requires a certain technology to be viewed will not be displayed correctly or completely by a browser that does not support that technology. For example, Firefox does not support ActiveX, which are software components from Microsoft that enable sound, Java applets, and animations to be integrated in a Web page.[21] For example, using a browser that supports ActiveX is necessary in order to access the Windows Update Web site, which otherwise will simply not be displayed but with an alert to the viewer that content is hidden from view. The fact that content is not being displayed or displayed in a different way from the original site is not always apparent.

The key to capturing an archived Web site as accurately and completely as possible is to examine the underlying code used to create and support the Web site to determine whether a browser is incompatible. This can be done by an examination of the source code for the initial page of the Web site. The entry point for the Web site usually includes language that will query and collect information from the browser and its computer system settings to determine the best method of providing the information from the site. For Web sites that use only standard html coding, the content and features of the site usually have the least variance across browsers. Where non-standard html coding is revealed, forensic experts capturing Web sites for litigation purposes may display the Web site with multiple browsers as a test to ensure that the display does not vary by browser and if variances are noted, capture the Web site with the browser that displays the most content.

ADMITTING INTERNET ARCHIVE DATA

Information obtained from reputable or government-sponsored online sources has generally been held admissible. For example, in *U.S. Equal Employment Opportunity Commission v. E.I. DuPont De Nemours & Co.*,[22] the defendant moved to exclude as an exhibit the printout of a table from the Web site of the US Census Bureau as inadmissible hearsay and lack of trustworthiness. The court denied the motion, stating that the hearsay exception for a public record applied. In addition, the court concluded that the printout was sufficiently authenticated under Federal Rules of Evidence 901(a) since it contained the "internet domain address from which the table was printed, and the date on which it was printed."[23] The court performed its own verification as well, noting that "[t]he Court has accessed the website using the domain address and has verified that the webpage printed exists at that location."[24] Similarly, printouts of data from other government-sponsored Web sites have been admitted over objection to the reliability of the information.[25]

Reported cases involving Web site captures from the Internet Archive are rare, even though *archive.org* is an important resource for litigators trying to establish prior representations or actions on Web sites. Significantly, in the few cases where challenges have been interposed to Internet Archive versions of Web pages, the evidence has been admitted over hearsay and authentication challenges.

The leading case for admission of archived Web sites from the Internet Archive is *Telewizja Polska USA, Inc. v. Echostar Satellite Corporation.*[26] The plaintiff in this case claimed that Echostar improperly had used the plaintiff's trademarks in "TV Polonia," a Polish-language television station, to sell subscriptions to the Dish Network satellite TV service after the contract allowing such marketing rights had expired in early 2001. Echostar argued that plaintiff had itself advertised that the Dish Network carried TV Polonia on its Web site after the marketing rights had expired and offered an exhibit of the plaintiff's Web site at various times in 2001 confirming this past Web site content. The plaintiff filed a motion *in limine* to bar Echostar from offering the exhibit on the grounds of double hearsay and lack of authentication. The court rejected these grounds and denied the motion, stating that "the contents of [plaintiff]'s website may be considered an admission of a party-opponent and are not barred by the hearsay rule."[27] In addition, the court relied on the affidavit of "Ms. Molly Davis, verifying that the Internet Archive Company retrieved copies of the websites as it appeared on the dates in question from its electronic archives."[28] The plaintiff "presented no evidence that the Internet Archive is unreliable or biased" or "denied that the exhibit represents the contents of its website on the dates in question" or otherwise "challenged the veracity of the exhibit."

AUTHENTICATION CONSIDERATIONS FOR ARCHIVED WEB SITES

The versions of Web sites and pages archived on Internet Archive can provide valuable and significant probative evidence in a variety of cases. To authenticate copies of prior versions of Web sites obtained from the Wayback Machine, a party proffering the evidence must show, under Federal Rules of Evidence 901(a) that the "matter in question is what its proponent claims." This can be done by producing the testimony, either orally or in written form, of the person who copied or supervised the copying of the archived Web site and the process followed to accomplish this task. In addition, the proponent must establish the general reliability of the copy.

The capture and use as evidence of archived Web site material must be approached with a full appreciation of three primary technical features and limitations that may affect the archived copy in order to respond to any challenges that may be raised to the completeness, reliability, and authenticity of the copy. For this reason, expertise in digital forensics, including the methods of forensic capture and documentation of the archived Web site proffered, may be recommended depending on the issue for which the archived Web site is being offered.

First, archived Web sites on the Internet Archive are compilations made over time. While the archived versions of Web sites are date- and time-stamped, the pages for each version of the Web site may not have been copied simultaneously. The Alexa crawler may take multiple passes at a Web site over the course of up to two days to try to capture the entire Web site. In short, due to bandwidth and storage constraints, all of the data on a Web site may not be captured at the same time. The Internet Archive explains that "Sites are usually crawled within 24 hours and no more than 48."[29]

Second, the archived versions of Web pages available through the Wayback Machine may not contain all of the content on each Web page that is captured. What you see is not always the complete story.

For example, when a Web site contains elements that require interaction with the originating host, copying that page for archiving breaks the necessary link with the original site, thereby reducing the functionality or eliminating entirely that particular element. The result is that the archived Web page or site has missing material, which may not be apparent or flagged for the viewer. Similarly, links originally enabled with a java script, which the Alexa crawl technology disables during the capture of the Web site or Web page, would no longer work.[30] The Internet Archive acknowledges: "Not all images are archived nor are retrievable from the original site. If they no longer exist on the original site then the images will not be available and not displayed within the archived pages."[31] Other types of coded content that the crawler technology does not capture include Flash enabled content, some photographic images, and some html coded content.

Moreover, content may not ever be captured if problem technology, such a password protected pages, or respectful technology, such as a robots.txt flag, is encountered. Additionally, even after the capture is completed, archived copies of Web sites may have content deleted if a robots.txt flag is added to the site or if a request for deletion is sent to the Internet Archive. Thus, the archived copy may show what was captured but not what was skipped or subsequently omitted.

Finally, depending on the technical sophistication of the Web site and its use of internal and outside linked material, the copy of the archived version of the Web site may not show links that existed on the Web site at the time of the original capture. Links that may have worked at the date of capture may be inactive because they simply no longer exist or are not in the archive library.

The links on archived Web sites may remain active but link to different material from that associated with the Web page at the time that it was archived. The linked material may be to current sites or to other stored link sites from a different time. Indeed, links may connect to current active sites and show *current* banner advertisements available at the site, rather than linking to sites as they existed at the date of capture. When the active links on archived Web sites pull information from the current site, the owner of the current Web site can track how many times the Wayback Machine is being queried for archived versions of the Web site. Logs of incoming IP addresses maintained by the server hosting the current Web site can reveal whether the incoming IP address originated with the Internet Archive.[32]

Alternatively, the working link may connect to sites or pages archived on the Wayback Machine around the time of the original Web site to which the link connected. The Internet Archive explains: "When you are surfing an incomplete archived site the Wayback Machine will grab the closest available date to the one you are in for the links that are missing. In the event that we do not have the link archived at all, the Wayback Machine will look for the link on the live web and grab it if available."[33] In short, the process of copying a Web site for archiving may result in changes to the extent that the archived Web site may not show accurately the links that existed at the time shown for the Web site storage date. The Alexa Internet crawler technology rewrites the original link code in html to re-direct links to current or stored links.

Determining whether the content on a linked site is contemporaneous with the archived version of the site or dates from another time may be critical. For example, establishing that a linked promotion to a site containing infringing material persisted after notification from the copyright owner may be important to establish knowledge and intent in a copyright infringement suit. Each link must be checked for the date code embedded in the archived URL, or location within the Wayback Machine database, to verify whether the linked content is contemporaneous, current, earlier or later than the version of the archived web site or page. The Internet Archive provides the following example: "in this url *http://web.archive.org/web/20000229123340/http://www.yahoo.com/* the date the site was crawled was Feb 29, 2000 at 12:33 and 40 seconds."[34]

Increasingly, documentation of offending activity that occurred on Web sites of opposing parties is relevant and, in some cases, dispositive of certain types of claims. Searching for, reviewing, and capturing archived copies of Web sites can be easily accomplished from the Internet Archive, but litigators should consider carefully the methods of capture and the issues surrounding the completeness, reliability, and authenticity of the Web site copies.

NOTES

[1] *See, e.g.*, Van Wetrienen v. Americontinental Collection Corp., 94 F. Supp. 2d 1087, 1109 (D. Or. 2000) (contents of defendant's Web site relevant to determination of whether defendant's conduct was so egregious as to merit an award of punitive damages).

[2] The CyberCemetery is located at *http://govinfo.library.unt.edu.*

[3] ERC is located at *http://dosfan.lib.uic.edu/ERC/.*

[4] The 2004 Presidential Term Web Harvest is located at *http://www.webharvest.gov/collections/peth04/.*

[5] *http://www.loc.gov/minerva/collect/elec2002/index.html.*

[6] *http://www.loc.gov/minerva/collect/sept11/index.html.*

[7] *http://www.loc.gov/minerva/collect/elec2000/index.html.*

[8] *See http://searchengineshowdown.com/stats/freshness.shtml.*

[9] The Internet Archive is located at *www.archive.org.*

[10] Kahle v. Ashcroft, 2004 U.S. Dist. LEXIS 24090, *5 (N.D. Cal. Nov. 19, 2004).

[11] *http://pages.alexa.com/company/technology.html.*

[12] *http://www.archive.org/about/faqs.php#The _Wayback_Machine.*

[13] *http://websearch.alexa.com/welcome.html.*

[14] *http://www.bibalex.org/english/initiatives/internetarchive/web.htm; see also http://en.wikipedia.org/wiki/Bibliotheca_Alexandrina.*

[15] The technical term for an Internet address is Universal Resource Locator or URL.

[16] Directions for removal of a Web site from the archive are found at *http://www.archive.org/about/exclude.php.*

[17] *http://www.archive.org/about/faqs.php#2* ("By placing a simple robots.txt file on your Web server, you can exclude your site from being crawled as well as exclude any historical pages from the Wayback Machine.").

[18] *Id.*

[19] Healthcare Advocates, Inc. v. Harding, Earley, Follmer & Frailey, Civil Action (E.D. Pa., filed July 8, 2005), copy at *http://www.geocities.com/bledrydudenet/Healthcare_Advocates_v._Harding_Complaint__FINAL.pdf.* Healthcare Advocates, Inc. unsuccessfully moved to have the counts against the law firm for, *inter alia*, violations of the DMCA and the Computer Fraud and Abuse statute added to the underlying complaint, but that motion was denied. Flynn v. Health Advocate, Inc., 2004 U.S. Dist LEXIS 12536, *12 (E.D. Pa. July 8, 2004).

[20] *http://www.archive.org/about/terms.php/.*

[21] *See http://webmaster.lycos.co.uk/glossary.*

[22] U.S. Equal Employment Opportunity Commission v. E.I. DuPont De Nemours & Co., 2004 U.S. Dist. LEXIS 20753 (E.D. La. Oct. 18, 2004).

[23] *Id.* at *5.

[24] *Id.*

[25] *See* Chapman v. San Francisco Newspaper Agency, 2002 U.S. Dist. LEXIS 18012 at*2 (N.D. Cal. Sept. 20, 2002) (computer printout of page from US Postal Service Web site was sufficiently reliable to be admissible public record). *But see* St. Clair v. Johnny's Oyster & Shrimp, Inc., 76 F. Supp. 2d 773, 774 (S.D. Tex. 1999) (court deemed plaintiff's proffered data from the US Coast Guard's online vessel database insufficient since "any evidence procured off the Internet is adequate for almost nothing").

[26] Telewizja Polska USA, Inc. v. Echostar Satellite Corp., 2004 U.S. Dist. LEXIS 20845 (N.D. Ill). *See also* Attig v. DRG, Inc., 2005 U.S. Dist. LEXIS 5183, at *5, n.1 (E.D. Pa. Mar. 30, 2005) (in copyright infringement suit, parties agreed that copies of websites at issue obtained from *archive.org* are admissible evidence); Louis Vuitton Malletier v. Burlington Coat Factory Warehouse Corp., 42 F.3d 532, 535 (2d Cir. 2005) (in trademark infringement suit, evidence of defendant's Web site advertisements presented through *archive.org* capture of the site content at particular time).

[27] *Id.* at *16-17.

[28] *Id.*

[29] *http://www.archive.org/about/faqs.php#The _Wayback_Machine.*

[30] *Id.* ("javascript enabled links and actions are disabled in the comparison results to prevent errant scripts from being run").

[31] *Id.*

[32] This feature of the Wayback Machine is what alerted Healthcare Advocates in the pending lawsuit discussed *supra*, at n.20 that prior versions of its Web site had not been blocked as requested but instead were being accessed by the defendants.

[33] *http://www.archive.org/about/faqs.php#The _Wayback_Machine.*

[34] *Id.*

The NSA's Interception of E-mails and Phone Calls
Continued from page 1

conference.[7] Attorney General Gonzales called the program "limited in scope" and said that "[t]his is a very concentrated, very limited program focused on getting information about our enemy."[8]

On December 24, however, the *New York Times* quoted current and former administration officials and telecommunications company managers as saying that several major US telecommunications companies had given the NSA access to the telecommunications switches[9] through which the companies routed international telephone calls and email traffic. Those officials and managers disclosed that the NSA uses the access to the switches not only to eavesdrop on specific conversations but also to comb through large volumes of telephone and Internet traffic to search for patterns that might point to terrorism suspects.[10]

The government and telecommunications officials told the *Times* that the NSA analyzes the "communications patterns to glean clues from details like who is calling whom, how long a phone call lasts and what time of day it is made, and the origins and destinations of e-mail messages."[11] A former telecommunications manager stated that "the real plum is going to be the transaction data and traffic analysis," which can be "used to identify lines of communication that are given closer scrutiny."[12] The data mined by the NSA reportedly includes calls and Internet traffic from one non-US country to another non-US country that are routed through telecommunications switches in the United States. The *Times* quoted a telecommunications engineer, Phil Karn: "If the government is gaining access to the switches like this, what you are really talking about is the capability of an enormous vacuum operation to sweep up data."[13]

While the details of the NSA surveillance remain classified, the December 16 and December 24 articles in the *New York Times* show that the NSA is doing at least three things:

1. It is monitoring calls and emails to and from certain "hot" telephone numbers and email addresses obtained when it captures Al Qaeda operatives with their cell phones, computers, and perhaps lists of contacts, or which it obtained from lawful foreign surveillance. While the NSA was undoubtedly monitoring communications to and from such telephone numbers and email addresses that were outside the United States before 9/11, after the 9/11 attacks it appears that the agency began monitoring communications to and from such numbers in the United States.
2. With the cooperation of several US telecommunications companies, the NSA has tapped into the companies' core switches in cities where the switches process large amounts of international telephone and email communications, then uses "sniffer" and filtering technology to identify calls and emails that merit further scrutiny.
3. The NSA is using software algorithms to analyze the large volume of communications data it is intercepting, probably together with commercially available data of all kinds, to determine if there are patterns that point to individuals, telephone numbers, or email addresses that should be individually monitored.

CONGRESSIONAL, JUDICIAL, AND COMMENTATORS' RESPONSES TO THE NSA PROGRAM

After the NSA began monitoring communications that began or ended in the United States, Bush administration officials secretly briefed selected congressional leaders about the program. Senator John D. "Jay" Rockefeller, IV, a Democrat from West Virginia, wrote a letter on July 17, 2003, to Vice President Cheney after he received such a briefing. Senator Rockefeller released a copy of the letter on December 19, 2005.[14] In the 2003 letter, Senator Rockefeller wrote in part:

> Given the security restrictions associated with this information, and my inability to consult staff or counsel, I feel unable to fully evaluate, much less endorse these activities.
>
> As I reflected on the meeting today, and the future we face, John Poindexter's TIA project sprung to mind, exacerbating my concern regarding the direction the Administration is moving with regard to security, technology and surveillance.[15]

Senator Rockefeller said that, after he sent the letter to Vice President Cheney, "these concerns were never addressed and, I was prohibited from sharing my views with my colleagues."[16]

Congresswoman Nancy Pelosi, Democrat from California, said that the briefings of Congressional Intelligence Committee members after the program began were notifications, not requests for approval. "As is my practice whenever I am notified about such intelligence activities, I expressed my strong concern during these briefings." [17] Her letter to then NSA Director Hayden and his response were recently declassified at her request and released.[18] Congresswoman Pelosi's October 11, 2001, letter expressed concerns about whether the NSA had legal authority for the surveillance it was conducting.

Former Senator Tom Daschle, who was majority leader of the Senate when the 2001 congressional resolution relied on by the Bush administration was passed, wrote that he negotiated with then White House counsel Alberto Gonzales regarding the language of the resolution.[19] The issue of warrantless wiretaps of US citizens never came up when he helped shepherd the resolution through the Congress. On the contrary, the White House asked that the phrase "in the United States and" be inserted in the resolution after the phrase "appropriate force."[20] He said that he rejected the proposed change because he "could see no justification for Congress to accede to this extraordinary request for additional authority."[21] Daschle wrote that Congress did not grant the authority to conduct the NSA operation that President Bush claims was granted in the congressional resolution.[22]

Senator Arlen Specter, Republican of Pennsylvania and Chair of the Senate Judiciary Committee, said that the committee would conduct hearings early this year regarding the NSA program. Senator Specter said that

> the Judiciary Committee will be interested in its oversight capacity to learn from the attorney general or others in the Department of Justice the statutory or other legal basis for the electronic surveillance, whether there was any judicial review involved, what was the scope of the domestic intercepts, what standards were used to identify Al Qaeda or other terrorist callers, and what was done with this information.[23]

Democratic Senators Carl Levin of Michigan, Jack Reed of Rhode Island, and Russell Feingold of Wisconsin criticized President Bush for by-passing the FISA court.[24]

After the data mining component of the NSA program was disclosed on December 24, Senator Patrick Leahy of Vermont, the ranking Democrat on the Judiciary Committee, said that "these new revelations can only multiply and intensify the questions and concerns about the warrantless surveillance of Americans."[25] An unnamed Republican congressional aide said that "[w]e want to look at the entire program, an in-depth review, and this new data-mining issue is certainly part of the whole picture."[26]

Most members of the FISA court reportedly learned about the NSA program when the *New York Times* disclosed it in mid-December.[27] One FISA Judge, James Robertson of the D.C. District Court, resigned his position on the FISA court to protest the NSA program.[28] The current Presiding Judge of the FISA court, Judge Colleen Kollar-Kotelly, also of the D.C. District Court, asked the Bush administration for a secret briefing on the NSA program.[29] Another FISA Judge, US District Court Judge Dee Benson of Utah said that "[t]he questions are obvious. What have you been doing and how might it affect the reliability and credibility of the information that we're getting in our court?"[30]

Presiding FISA Judge Kollar-Kotelly reportedly helped trigger a suspension of the NSA program in mid-2004 when she raised concerns about whether information gained through the program was being used as a basis for FISA warrant requests.[31] Government lawyers said that "there appeared to be concerns that the Justice Department, by trying to shield the existence of the NSA program, was in danger of misleading the court about the origins of the information cited to justify the warrants."[32]

Judge Richard A. Posner, a well-known judge on the Seventh Circuit and a senior lecturer in law at the University of Chicago, wrote that the FISA requirement that US citizens or lawful residents must be shown to be involved in hostile acts before surveillance is authorized is too restrictive.[33] Data mining that involves computerized sifting of data from innocent people should be allowed, he wrote, because machine collection and sifting of data cannot invade privacy and the data may contain valuable counter-terrorist information.[34]

Other commentators agree with Judge Posner that FISA should be revised to permit data mining. Referring to the data mining aspect of the NSA program described in the December 24 the *New York Times* story, one writer stated:

> The heart of the program may be this effort to find links and patterns. William Arkin described in a Dec. 23 posting to his washingtonpost.com column, Early Warning, how the data-mining process might work: "Massive amounts of collected data—actual intercepts of phone calls, e-mails, etc.,—together with transaction data—travel or credit card records or telephone of Internet service provider logs—are mixed through a mind-boggling array of government and private sector software programs to look for potential matches.
>
> This is the kind of technology we should be using, with appropriate safeguards. . . .
>
> America's best intelligence asset is technology. The truth is that America has never been especially good at running spies or plotting covert actions. Our special talent has been the application of technology to complex problems of surveillance. . . .
>
> America needs surveillance and analytical techniques that can connect the dots. But even more, it needs a clear legal framework for this effort. Otherwise it won't be sustainable. In that sense, continuing the current lawless approach would be the true gift to the enemy.[35]

Such reliance on technology is not shared by all US intelligence professionals.[36] It is apparent, however, that deploying technological tools is an important part of the US response to the Al Qaeda threat.

PREVIOUS FEDERAL DATA MINING PROJECTS AND CONGRESSIONAL RESPONSES

The term "data mining," is generally accepted to mean "the iterative process of detecting and extracting . . . patterns from large databases."[37] Data mining technology "facilitates the ability to sort through masses of information through database exploration, extract specific information in accordance with defined criteria, and then identify patterns of interest to its user."[38]

The fundamentals of data mining are based on statistical methods, such as Bayesian algorithms, that have been refined over the past 40 years.[39] With the increase in computing power and the advent of the Internet, it has become possible to mine larger data sets than were imaginable only a few years ago. Companies such as Acxiom, Seisint (now a part of LexisNexis), Equifax, Experian, Trans Union, SPSS, and Quadstone have made available tools and databases that allow private entities to perform incredibly detailed analyses of their data. Commentators have noted that Acxiom has "more information on Americans than the Internal Revenue Service"[40] and that Acxiom's data warehouse can hold a petabyte of information (the equivalent of "a 50,000-mile high stack of King James Bible").[41] Acxiom's Consumer Infobase is a database that contains information on "over 150 million individuals residing in over 100 million households" in the United States.[42] Seisint has developed "a digital identity system that somehow managed to tag every adult American citizen with a unique code."[43] Data mining technology is rapidly evolving. More advanced algorithms for massaging and managing data are regularly deployed to replace or supplement those developed over the past few years.

Although data mining had its genesis in the private sector,[44] it has become a crucial tool in the law enforcement community since the attacks of September 11.[45] Federal and state agencies have worked closely with private companies such as Acxiom and Seisint to use the databases and computing abilities of these companies for programs such as MATRIX (the Multi-state Anti-Terrorism Information Exchange).[46] MATRIX was developed by Seisint within weeks after the September 11 attacks and soon after Seisint had demonstrated to federal and state law enforcement officials its ability to use data mining to identify the hijackers who had commandeered the planes.[47] Acxiom similarly demonstrated the same ability to law enforcement officials soon after the September 11 attacks.[48]

Even prior to the September 11 attacks, state and federal agencies relied on data mining techniques to identify criminal activity, fraudulent misuse of governmental credit cards, and Medicaid and Medicare abuse.[49] After the September 11 attacks, however, government agencies have relied more heavily on data mining technologies and databases maintained by companies such as Acxiom and Seisint.[50] For example, according to the Electronic Privacy Information Center, in 2002 the "Department of Justice obtained a $11,000,000 contract for access to ChoicePoint databases" and the Immigration and Naturalization Service (now part of the Department of Homeland Security) "queries private sector databases 20,000 times a month."[51] When it adopted the Homeland Security Act in 2002,[52] Congress encouraged the newly formed Homeland Security Department to work with intelligence agencies, including the NSA and CIA, to establish and use "data-mining and other advanced analytical tools."[53] The Department of Defense proposed a number of data mining programs, including the Total Information Awareness (TIA) program[54] and the Department of Homeland Security proposed the Computer Assisted Prescreening Process System II (CAPPS II). In 2003, Congress held a number of hearings regarding these programs.[55] TIA was cancelled as a result of the public outcry that followed release of its details,[56] and CAPPS II was replaced by the Secure Flight program.[57]

The federal government has continued its data mining efforts despite a conclusion by the Defense Advanced Research Projects Agency that "the existing data mining approach of discovering previously unknown patterns is ill-suited to ferreting out terrorist plans."[58] Federal agencies continue to rely on publicly available data sources despite recognition "that public source data is not always accurate. In fact, many times there are errors."[59]

Data mining efforts by federal agencies are governed by the Privacy Act of 1974,[60] the Computer Matching and Privacy Protection Act of 1988,[61] and the E-Government Act of 2002.[62] Additionally, local, county, state, and federal agencies that receive and submit criminal intelligence information are subject to the Criminal Intelligence Systems Operating Policies.[63] Exemptions in the laws have freed law enforcement agencies from many of the constraints of the acts.[64] For example, in 2003 the FBI announced a final rule exempting its National Crime Information Center, Central Record System, and National Center for the Analysis of Violent Crime from the Privacy Act.[65] In particular, the FBI exempted its databases from the Privacy Act's requirement that agencies ensure the "accuracy, relevance, timeliness, and completeness" of their systems of record.[66] When questioned about this final rule by a congressional subcommittee, an FBI official explained that those system of records needed to be exempted so that leads that upon further inquiry turn out to be false could still be maintained in the databases (along with a clarification that the lead had turned out to be false).[67]

STATUTORY AND CONSTITUTIONAL RESTRICTIONS ON NSA SURVEILLANCE

President Truman created the NSA by a top secret order in 1952.[68] The federal government did not list the agency in its public directories before 1962.[69] Executive Order 12333, last amended in January 2003, describes in § 1.12(b) the NSA's responsibilities.[70] One of the NSA's missions is to acquire information from electronic signals and to distill that information for assimilation by the intelligence community and national policymakers.[71] As a part of its "signals intelligence" or SIGINT activity, NSA surreptitiously intercepts international electronic communications by a variety of means, all of which it tries to keep secret.[72]

A declassified copy of the NSA's 2001 "Transition" document reveals that, in 2000 and 2001, the agency was moving away from its past SIGINT methods to monitor communications on the global digital, telecommunications network:

> In the past, the NSA operated in a mostly analog world of point-to-point communications, carried along discrete, voice channels. . . .
>
> Now, communications are mostly digital, carry billions of bits of data, and contain voice, digital, and multimedia data. . . . The volumes and routing of data make finding and processing nuggets of intelligence information more difficult. To perform both its offensive and defensive missions, NSA must "live on the network."
>
> This new approach is well under way. Significant effort and investment are being applied to master the global network, both to protect our nation's communications and to exploit those of our targets.
>
> . . .
>
> [B]ecause of the communications environment described above, availability of critical foreign intelligence information will mean gaining access in new places and in new ways. . . . [Material redacted by the NSA.]
>
> NSA can and will perform its missions consistent with the Fourth Amendment and all applicable laws. But senior leadership must understand that today's and tomorrow's mission will demand a permanent, powerful presence on a global telecommunications network that will host the "protected" communications of Americans as well as the targeted communications of adversaries.[73]

From the December 24 New York Times report, it appears that, beginning in late 2001 or early 2002, the NSA gained access to at least some parts of the "global communications network" that it referred to in its Transitions 2001 report when US telecommunications companies voluntarily gave the agency access to switches located in the United States.

THE LEGAL JUSTIFICATIONS CITED BY THE BUSH ADMINISTRATION FOR THE NSA PROGRAM

The Bush administration apparently received classified legal opinions from Justice Department lawyers prior to initiating the NSA program that asserted that the President has constitutional authority as Commander in Chief under the US Constitution to authorize the program as well as congressional authorization from the resolution passed in response to the September 11 attacks.[74] After President Bush confirmed that the *New York Times* description of the NSA program was essentially accurate, the Justice Department sent a letter to the Chairpersons and ranking minority members of the House and Senate Intelligence Committees that explained the administration's legal justification for the NSA program.[75] In the letter, the Department argues that the President has inherent constitutional authority under Article II of the Constitution, including his authority as Commander in Chief, to authorize the NSA program to fulfill his duty to protect the nation from further attacks.[76] The Department also argues that the President has authority to order NSA to implement the program pursuant to the AUMF. The Department's letter asserts that the President's "constitutional authority includes the authority to order warrantless foreign intelligence surveillance within the United States, as all federal appellate courts, including at least four circuits to have addressed the issue have concluded."[77]

The Department's position is essentially that the President's inherent constitutional authority to direct the NSA to conduct warrantless electronic surveillance within the United States was supplemented by "statutory authority under the AUMF." The Department argues that the Supreme Court's decision in *Hamdi v. Rumsfeld*,[78] in the plurality opinion of Justice O'Connor and in the dissenting opinion of Justice Thomas, held that the AUMF authorized the "fundamental incident[s] of waging war," including, in the *Hamdi* case, the "detention to prevent a combatant's return to the battlefield." The Department claims that "communications intelligence activities" constitute "a fundamental incident of waging war" and therefore are similarly authorized by the AUMF. The Department's letter also argues that "the President's inherent 'authority is at its maximum'" under the standards stated in Justice Jackson's concurrence *Youngstown Sheet & Tube Co. v. Sawyer.*[79] The Department argues that the statutory authorization in the AUMF makes the NSA surveillance lawful under FISA by providing the statutory exception referred to in section 109 of FISA.[80]

The Department of Justice further argues that the NSA's activities are consistent with the Fourth Amendment and with the protection of civil liberties. The Department's letter claims that the NSA program meets the Fourth Amendment's central requirement of reasonableness and falls within the "special needs" cases that justify a departure from the usual requirement that a warrant be issued before a search is conducted.[81] The Department argues that "[i]ntercepting communications into and out of the United States of persons linked to al Qaeda in order detect and prevent a catastrophic attack is clearly *reasonable.*" (Emphasis in original.)

Finally, the Department argues that "the President determined that it was necessary following September 11 to create an early warning detection system. FISA could not have provided the speed and agility required for the early warning detection system."

THE CONGRESSIONAL RESEARCH SERVICE DISPUTES THE ADMINISTRATION'S LEGAL JUSTIFICATIONS

On Thursday, January 5, 2006, the Congressional Research Service (CRS) released a 44-page memorandum that responds to each of the Department's arguments.[82] The CRS is the "public policy research arm of the United States Congress."[83] Congress created the CRS "to have its own source of nonpartisan, objective analysis and research on all legislative issues."[84]

The CRS memo states that Congress intended the procedures of FISA to "be the exclusive means by which electronic surveillance . . . and the interception of domestic wire, oral, and electronic communications may be conducted."[85] After addressing the justifications in the Department's letter in detail, the CRS memo states that, "[i]f the NSA operations at issue are encompassed in the definition of 'electronic surveillance' set forth under FISA, it would seem consistent with Congress's intent that such surveillance must be carried out in accordance with the FISA procedures."[86]

The CRS authors reject the Department of Justice's argument that the AUMF implicitly amended FISA to permit the NSA to conduct those parts of its program that would otherwise violate FISA.[87] The authors conclude that "the Administration's legal justification, as presented in [the December 22 letter], does not seem to be as well-grounded as the tenor of the letter suggests."[88]

The CRS's analysis is thorough and persuasive. It understates, however, the weaknesses of some of the administration's arguments. For example, Justice O'Connor's plurality opinion in *Hamdi*, which the Department relies on in its letter, includes the holding that "the indefinite detention [of unlawful combatants] for the purpose of interrogation is not authorized."[89] Indefinite detention of an Al Qaeda combatant for the purpose of interrogation plainly resembles indefinite electronic surveillance for the same purpose. If the AUMF does not authorize the former, as Justice O'Connor wrote, then neither does it authorize the latter.[90] Further, the Department's argument that "communications intelligence targeted at the enemy is a fundamental incident of the use of military force" sidesteps the issue. It is beyond debate that the President has such authority generally; the issue is whether the AUMF authorized such intelligence within the United States, including intercepts of communications to and from US persons, notwithstanding the prohibition in section 109 of FISA.

As for the Department's and the President's claim that exigent circumstances required electronic surveillance to be conducted without getting FISA Court orders, FISA permits surveillance without a FISA court order for 72 hours, provided that the Attorney General or his designee notifies the FISA court within the 72-hour period and seeks a retroactive FISA court order.[91] The Bush administration has not answered questions about why the administration did not use this temporary authority under FISA rather than ignoring FISA altogether.

In addition to the compelling arguments in the CRS memo responding to the Department's claim that the President has inherent power derived from his position as Commander in Chief in Article II of the Constitution notwithstanding FISA § 109,[92] it should be noted that the Department's analysis relies on language in the FISA court of review opinion regarding the President's inherent authority to conduct warrantless searches to obtain foreign intelligence that is plainly *dicta*. The issue decided by the FISA court of review in *In re Sealed Case* was whether or not the supposed "wall" between criminal and intelligence functions within the Department of Justice had to be continued despite opposition and the Patriot Act's elimination of the "primary purpose" test. The court of review held that the Patriot Act permitted newly-promulgated Department of Justice procedures that allowed unrestricted sharing of intelligence information with criminal prosecutors.[93] The language in the decision regarding the President's inherent authority to conduct warrantless searches was unnecessary to the decision in the case.

Finally, the CRS notes that FISA (1) explicitly repealed the former section of Title III of the Omnibus Crime Control and Safe Streets Act that authorized electronic surveillance for certain classes of crimes but specifically stated that it did not "limit the constitutional power of the President . . . to obtain foreign intelligence information," and (2) replaced that non-interference clause with § 109 of FISA, which explicitly restricts executive branch's authority to conduct foreign intelligence surveillance to the procedures set forth in FISA.[94] But the CRS did not clearly state that the conflict between FISA's requirements and the Department's claim that the President has inherent powers to conduct the surveillance should be resolved pursuant to the standards stated in category three from Justice Jackson's concurring opinion in *Youngstown Sheet & Tube Co.*[95] Justice Jackson described that category as follows:

> When the President takes measures incompatible with the expressed or implied will of Congress, his power is at its lowest ebb, for then he can rely only on his constitutional powers minus any constitutional powers of Congress over the matter. Courts can sustain exclusive Presidential control in such a case only by disabling the Congress from acting upon the subject.[96]

The contending claims should be resolved under Justice Jackson's category three standard.

The Department implies that the President has *exclusive* authority over foreign intelligence operations such that the executive branch may ignore the restriction in § 109 of FISA. It seems unlikely that such argument would be successful. In *Hamdi*, both Justice O'Connor in the plurality decision and Justice Souter in his concurring opinion rejected the Justice Department's argument that the President had exclusive powers to determine whether unlawful combatants could be detained indefinitely:

> In so holding, we necessarily reject the Government's assertion that separation of powers principles mandate a heavily circumscribed roll for the courts in such circumstances. Indeed, the position that the courts must forego any examination of the individual case and focus exclusively on the legality of the broader detention scheme cannot be mandated by any responsible view of separation of powers, as this approach serves only to condense power into a single branch of government. We have long since made clear that a state of war is not a blank check for the President when it comes to the rights of the Nation's citizens. Youngstown Sheet & Tube, 343 U.S. at 587. Whatever power the United States Constitution envisions for the Executive in its exchanges with other nations or with enemy organizations in times of conflict, it most assuredly envisions a role for all three branches when individual liberties are at stake.[97]

Unless the appointment of Chief Justice Roberts, the pending resignation of Justice O'Connor, and the appointment of Judge Samuel Alito changes the Supreme Court's views on this issue in a way that causes the court to radically departs from the analysis in *Youngstown Sheet & Tube*, any claim by the administration that it has exclusive authority over foreign intelligence electronic surveillance within the United States would likely be rejected.

The Department's arguments regarding the Fourth Amendment are also problematic for reasons in addition to those described by the CRS.[98] While the exigent circumstances immediately after the 9/11 attacks made it reasonable for the intelligence community to take whatever actions it could to determine who launched the attacks and whether or not more attacks were imminent,[99] it is an open question whether it remains reasonable more than four years after the attacks to take similar actions outside of the congressionally mandated structure of FISA. Further, if the reports that the NSA is intercepting all calls and emails that pass through certain telecommunications switches in the United States are accurate and if the NSA is mining those data together with extensive commercial data obtained from various US companies, it is debatable, if not doubtful, that such pervasive monitoring of communications by US citizens and lawful residents would be found reasonable under the Fourth Amendment.

THE NSA'S INTERCEPTS AT US TELECOM SWITCHES WERE "ELECTRONIC SURVEILLANCE"

The CRS authors state that their conclusions are dependent on determining whether the NSA intercepts fall within FISA's definition of "electronic surveillance."[100] FISA defines "electronic surveillance" to include:

> (1) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire or radio communication sent by or intended to be received by a particular, known United States person who is in the United States, if the contents are acquired by intentionally targeting that United States person, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes;
>
> (2) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire communication to or from a person in the United States, without the consent of any party thereto, if

> such acquisition occurs in the United States . . . .
>
> (3) the intentional acquisition by an electronic, mechanical, or other surveillance device of the contents of any radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and if both the sender and all intended recipients are located within the United States; or
>
> (4) the installation or use of an electronic, mechanical, or other surveillance device in the United States for monitoring to acquire information, other than from a wire or radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes.[101]

Additionally, FISA defines "United States person" to include "a citizen of the United States, an alien lawfully admitted for permanent residence."[102] "Wire communication" is defined "any communication while it is being carried by a wire, cable, or other like connection furnished or operated by any person engaged as a common carrier in providing or operating such facilities for the transmission of interstate or foreign communications."[103]

The *New York Times* articles disclose that the NSA intentionally intercepted telephone calls and emails with one end-point in the United States at telecommunications switches in the United States, searched the contents of some intercepted calls and messages for key words, and analyzed transaction data from others.[104] For the NSA to use sniffer and filtering programs on words that are part of the contents of messages and to analyze transaction data, the NSA has to intercept both the contents of and the transaction data regarding the communications.

If the reports from the *Times* are accurate, the NSA's intentional interception of the *contents* of communications to known targets is electronic surveillance as described in 50 U.S.C. § 1801(f)(1) and the wholesale interception of all traffic from communications switches in the United States, many of which emails and telephone calls were to or from persons in the United States, is electronic surveillance as described in 50 U.S.C. § 1801(f)(2). Nothing in the legislative history of 50 U.S.C. § 1801 suggests that the NSA was exempt from FISA when, after 9/11, it expanded its interception of non-US to non-US communications to intentionally intercept communications that began or ended in the United States.

The CRS memo points out that the legislative history of 50 U.S.C. § 1801 states that it was "designed to make clear that the legislation does not deal with international signals intelligence as currently [i.e., in 1978] engaged in by the National Security Agency . . . ."[105] The Senate Report that accompanied the bill enacted as FISA states that "[t]he nature of the National Security Agency activities, the purposes of such activities, and the technological problems associated with such activities have been carefully documented by the Church Committee . . . ."[106] The activities described in the cited sections of the Church Committee reports, other than those specifically criticized by the Committee, refer to the NSA's interception of non-US to non-US letters and telegrams; the Committee specifically condemned the NSA's intentional interception of communications to or from "Americans" in the United States.[107] The NSA's intentional interception of both the content and transaction data of all telephone calls and emails at telecommunications switches in the United States is different from the approved NSA programs that existed when FISA was enacted, which were excluded from FISA's definition of "electronic surveillance."

CONCLUSION

The Department of Justice's arguments that the NSA program did not violate FISA are unpersuasive. Its argument that the President has inherent constitutional authority to ignore FISA and its argument that FISA was implicitly amended by the AUMF appear flawed as well. If the *New York Times*' reports regarding the NSA's interception of calls and emails at telecommunications switches in the United States are accurate, the Department's contention that the surveillance does not violate the Fourth Amendment is, at best, doubtful.

Congress should carefully scrutinize the NSA program to assure that it is brought within the terms of FISA and to assure that it complies with the Fourth Amendment. This can be accomplished by amending FISA and by assuring that the NSA's surveillance does not unreasonably intrude on the privacy rights of US citizens and lawful residents.

NOTES

1. James Risen and Eric Lichtblau, "Bush Lets U.S. Spy on Callers Without Courts," *N.Y. Times*, Dec. 16, 2005, A1.
2. The FISA court was established in 1978 to review requests by the federal government to conduct surveillance of persons in the United States suspected of having ties with foreign intelligence agencies or with terrorists. *See* the Foreign Intelligence Surveillance Act, Pub. L. 95-511, 92 Stat. 1796 (1978), *codified at* 50 U.S.C. §§ 1801-1811. FISA was enacted after NSA surveillance of US citizens was brought to light by a Senate Judiciary Committee's investigation in the 1970s led by Senator Frank Church. *See* S. Rep. No.755, 94th Cong., 2d Sess. 736 (Gov't. Printing Office 1976), Book III, *Supplementary Detailed Staff Reports on Intelligence Activities and the Rights of Americans. See also* James Bamford, "The Agency That Could Be Big Brother," *N.Y. Times*, Dec. 25, 2005, Section 4, pp.1, 4. The FISA court may authorize surveillance of a foreign power or its agents only if the Attorney General approves the application and the application identifies the target of the surveillance, states facts that show that the target is a foreign power or agent of a foreign power, and a national security official certifies that a significant purpose of the of the surveillance is to obtain

foreign intelligence information. 50 U.S.C. § 1804(a)(7). The FISA court may not authorize the requested surveillance unless it finds probable cause to believe that the target is a foreign power or an agent of a foreign power and finds that foreign intelligence information is being sought. 50 U.S.C. §§ 1805(a)(3), (5). "Agent of a foreign power" is defined to include any person who "knowingly engages in sabotage or international terrorism, or activities that are in preparation therefore, for or on behalf of a foreign power." 50 U.S.C. § 1801(b)(2)(C). The term has been held to include terrorists, such as those who bombed the World Trade Center in 1993. United States v. Rahman, 861 F. Supp. 247 (S.D.N.Y. 1994), *aff'd*, 189 F.3d 88 (2d Cir. 1999), cert. denied, 528 U.S. 982 (1999). Since 1979, the 11-member FISA court has approved at least 18,740 applications for electronic surveillance or physical searches. Stewart M. Powell, "Secret Court Modified Wiretap Requests," *Seattle Post-Intelligencer*, Dec. 24, 2005, A1. The court modified only two of 13,102 proposed orders in the first 22 years that it reviewed them, but modified 179 since 2001, including 173 in 2003-2004. *Id.* It also reportedly denied or deferred six applications in 2003-2004, though it had not previously denied or deferred any applications. *Id.*

3. James Risen and Eric Lichtblau, *supra* n.1.
4. *Id.*
5. *Id.*
6. David Sanger, "Bush Says He Ordered Domestic Spying," N.Y. *Times*, A1.
7. Eric Lichtblau and David Sanger, "Administration Cites War Vote in Spying Case," N.Y. *Times*, Dec. 20, 2005, A1.
8. *Id.*
9. In a telecommunications network, a switch is a device that channels incoming data from multiple input ports to specific output ports that will take the data toward their intended destination. Switches are located, among other places, at the backbone levels of a network where one network connects with another. Such switches are often known as "core switches." In the traditional, circuit-switched telephone network, one or more switches set up dedicated, temporary connections or circuits for exchanges between two or more parties. In a wide-area, packet-switched network such as the Internet, switches determine from the IP address in each packet the output port to use for the next part of a packet's trip to the intended destination. Most data today are sent using digital signals over networks that use packet-switching. *See* the definition of "switch" at *http://whatis.techtarget.com* (last accessed Jan. 10, 2006).
10. James Risen and Eric Lichtblau, "Spy Agency Mined Vast Trove, Officials Report," N.Y. *Times*, Dec. 24, 2005, A1.
11. *Id.*
12. *Id.*
13. *Id.*
14. Eric Lichtblau and David Sanger, *supra* n.7.
15. A copy of the letter is available at *http://www.npr.org/documents/2005/dec/rockefeller.pdf* (last accessed Jan. 10, 2006).
16. Eric Lichtblau and David Sanger, *supra* n.7.
17. David Sanger, *supra* n.6.
18. The letters are available at *http://www.house.gov/pelosi/press/releases/Jan06/declassified.html* (last accessed Jan. 6, 2006).
19. Tom Daschle, "Power We Didn't Grant," *Wash. Post*, Dec. 23, 2005, A21. The resolution is referred to as the "Authorization for Use of Military Force" (AUMF), Pub. L. 107-40, 115 Stat. 224 (September 18, 2001). The resolution authorized the President "to use all necessary and appropriate force against those nations, organizations, or persons he determined planned, authorized, committed, or aided the terrorist attacks that occurred on Sept. 11, 2001, or harbored such organizations or persons, in order to prevent any future acts of international terrorism against the United States by such nations, organizations, or persons."
20. *Id.*
21. *Id.*
22. *Id.*
23. David Sanger, *supra* n.6.
24. Eric Lichtblau and David Sanger, *supra* n.7.
25. Eric Lichtblau, "Officials Want to Expand Review of Domestic Spying," N.Y. *Times*, Dec. 24, 2005, A20.
26. *Id*
27. Carol D. Leonnig and Dafna Linzer, "Judges on Surveillance Court to Be Briefed on Spy Program," *Wash. Post*, Dec. 22, 2005, A01.
28. *Id.* He will remain as a district court judge.
29. *Id.*
30. *Id.*
31. James Risen and Eric Lichthlau, *supra* n.1. The review of the program was also apparently prompted in part by the initial refusal of James Comey, Attorney General Ashcroft's top deputy in March 2004, to approve central parts of the program. Eric Lichtblau and James Risen, "Justice Deputy Resisted Parts of Spy Program," N.Y. *Times*, Jan. 1, 2006, A1. Mr. Comey was Acting Attorney General at the time due to Attorney General Ashcroft's hospitalization.
32. Risen and Lichtblau, *supra* n.1.
33. Richard Posner, "Our Domestic Intelligence Crisis," *Wash. Post*, Dec. 21, 2005, A31.
34. *Id.*
35. David Ignatius, "Eavesdropping and Evading the Law," *Wash. Post*, Dec. 28, 2005, A21.
36. *See, e.g.*, Floyd L. Paseman, A Spy's Journey, A CIA Memoir 285-86 (Zenith Press 2004): "9/11 was an intelligence failure. . . . We must not only maintain our overseas presence, we must increase it with properly qualified and trained personnel. . . . Spying is still best done on the ground overseas." Mr. Paseman spent 35 years as a CIA spy, 20 years overseas. *Id.*, 281. *See also* The 9/11 Commission Report 415, 535 n.43 (Norton 2004), *available at http://www.9-11commission.gov/report/911Report.pdf* (last accessed Jan. 9, 2006): "Recommendation: The CIA Director should emphasize . . . (b) transforming the clandestine service by building its human intelligence capabilities . . . ." "It is also notable that virtually all the information regarding possible domestic threats came from human sources. Information on overseas threats came from signals intelligence. Officials believed that signals intelligence was more reliable than human intelligence. . . ."
37. Jesus Mena, Data Mining Your Website 5 (Digital Press 1999).
38. Prepared Statement of Mark A. Forman, Associate Director for Information Technology and E-Government, Office of Management & Budget, Hearing Before the Subcommittee on Technology, Information Policy, Intergovernmental Relations & Census on Mar. 25, 2003 (March 25 Hearing), Serial No. 108-11 at 26.
39. *See, e.g.*, Mehmed Kantardzic, Data Mining: Concepts, Models, Methods, and Algorithms (IEEE Press 2003) (generally describing the mathematical and statistical tools used in data mining algorithms and the problems posed by large data sets); Prepared Statement of Jen Que Louie, President, Nautilus Systems, Inc., March 25 Hearing, *supra* n.38 at 19-21 (discussing tools used in data mining).
40. Mena, *supra* n.37 at 229-230.
41. Robert O'Harrow, Jr., No Place to Hide 37 (Free Press 2005).
42. Mena, *supra* n.37 at 230.
43. O'Harrow, *supra* n.41 at 106-107.
44. *See e.g.*, Mena, *supra* n.37 at 7-8.
45. *See generally* Robert O'Harrow, Jr., *supra* n.41.
46. *Id.* at 104-108. *See also* William J. Krouse, "The Multi-state Anti-Terrorism Information Exchange (MATRIX) Pilot Project," Cong. Res. Serv., Aug. 18, 2004.
47. *Id.* at 98-108.
48. *Id.* at 56-58.
49. Testimony of Florida State Senator Paula Dockery, March 25 Hearing, *supra* n.39 at 8-9; Prepared Statement of Mark Forman, *id.* at 28-30; Testimony of Gregory Kutz, Director, Financial Management and Assurance, General Accounting Office [now General Accountability Office], *id.* at 32-33.
50. Testimony of Senator Dockery.
51. EPIC Letter Re: Hearing on Data Mining: Current Application and Future Possibilities dated March 25, 2003, March 25 Hearing, *supra* n.38 at 90-91.
52. Pub. L. 107-296, 116 Stat. 2135 (2002), codified principally at 6.U.S.C. § 121.
53. 6 U.S.C. §§ 121(d)(14), 121(f)(B) and (D).

54. *See generally* Gina Marie Stevens, "Privacy: Total Information Awareness Programs and Related Access, Collection, and Protection Laws," Cong. Res. Serv. (Mar. 21, 2003).

55. *See, e.g.*, March 25 Hearing, *supra* n.39; Hearing Before the Subcommittee on Technology, Information Policy, Intergovernmental Relations & Census on May 6, 2003 (May 6 Hearing), Serial No. 108-72.

56. Pub. L. 108-87, Defense Appropriations Act of 2004 (Sept. 30, 2003). Section 8131(a) of that Act, however, included an exception for expenditures for "[p]rocessing, analysis, and collaboration tools for counterterrorism foreign intelligence."

57. TSA Press Release dated Aug. 26, 2004, *available at http://www.tsa.gov/public/display?content=09000519800c6c77* (last accessed Jan. 5, 2006).

58. Prepared Statement of Dr. Tony Tether, Director, DARPA, May 6 Hearing, *supra* n.55 at 51-52.

59. Testimony of Steven C. McCraw, Assistant Director, Office of Intelligence of the FBI, May 6 Hearing, *supra* n.55 at 14.

60. Pub. L. No. 93-579, 88 Stat. 1873 (codified at 5 U.S.C. § 552a).

61. Pub. L. No. 100-503, 102 Stat. 2507 (codified at 5 U.S.C. § 552a).

62. Pub. L. No. 107-347, 116 Stat. 2899.

63. 28 C.F.R. Part 23.

64. *See* Gina Marie Stevens, *supra* n.54 at 6-7.

65. Privacy Act of 1974, Implementation, 68 Fed. Reg. 14140 (Mar. 24, 2003) (amending 28 C.F.R. Part 16).

66. *Id.* (referring to 5 U.S.C. § 552a(e)(5)).

67. Testimony of Steven C. McCraw, May 6 Hearing, *supra* n.55 at 22.

68. Memorandum from President Harry S. Truman to the Secretary of State and the Secretary of Defense, "Communications Intelligence Activities" (Oct. 24, 1952). *See* S. Rep. No.755, 94th Cong., 2d Sess. 736 (1976); and H.R. Rep. 100-153(II), 100th Cong., 1st Sess. 3173, 3197 n.22 (1987), 1987 WL 61514. The NSA is a separately organized agency within the Department of Defense and is controlled by the Secretary of Defense.

69. H.R. Rep. 100-153(II), 100th Cong., 1st Sess. 3173.

70. Exec. Order No. 12333, 46 Fed. Reg. 59,941 (1981), *reprinted as amended in* 50 U.S.C. § 401 (note).

71. *Id.*, § 1.12(b)(1), (3); and Church of Scientology v. NSA, 610 F.2d 824, 825 (D.C. Cir. 1979)

72. Linder v. NSA, 94 F.3d 693, 696 (D.C. Cir. 1996).

73. National Security Agency and Central Security Service, "Transition 2001," Dec. 2000, 31-32, *available at http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB24/nsa25.pdf* (emphasis added) (last accessed Jan. 5, 2006).

74. Eric Lichtblau and David Sanger, *supra* n.7. John Yoo, then an official in the Justice Department's Office of Legal Counsel, reportedly worked on at least one of the legal opinions. *Id.* Mr. Yoo was one of attorneys at the Department who helped draft the USA Patriot Act, Pub L. No. 107-56, 115 Stat. 272 (2001) (codified as amended in various sections of the U.S.C.). Tim Golden, "Domestic Surveillance: The Advocate; A Junior Aide Had a Big Role in Terror Policy," N.Y. *Times*, Dec. 23, 2005, A1.

75. Available at *http://www.nationalreview.com/pdf/12%2022%2005%20NSA%20letter.pdf* (last accessed Jan. 5, 2006).

76. The Department cites Prize Cases, 67 U.S. (2 Black) 635, 668 (1863); and Campbell v. Clinton, 203 F.3d 19, 27 (D.C. Cir. 2000) (Silberman, J., concurring).

77: Citing In re Sealed Case, 310 F.3d 717, 742 (FISA Ct. of Review 2002).

78. Hamdi v. Rumsfeld, 542 U.S. 507 (2004). The court held in *Hamdi* that due process required that a US citizen captured in Afghanistan allegedly fighting for the Taliban had to be given a meaningful opportunity to challenge the factual basis for his detention as an unlawful combatant.

79. Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579, 635 (1952) (Jackson, J., concurring). The court held in *Youngtown* that President Truman did not have inherent constitutional authority to seize steel mills that were critical to the producing materials for the Korean War to prevent a strike from interfering with the war effort.

80. Section 109 is codified at 50 U.S.C. §§ 1809(a). It states in pertinent part: "A person is guilty of an offense if he intentionally—(1) engages in electronic surveillance under color of law except as authorized by statute . . . ." In other words, with certain exceptions, "electronic surveillance of a foreign power or its agents may not be conducted unless the FISA Court authorizes it advance." ACLU Foundation of S.Cal. v. Barr, 952 F.2d 457, 461 (D.C. Cir. 1991). The Department's December 22 letter discusses section 109 of FISA at pp.3-4.

81. Citing Illinois v. McArthur, 531 U.S. 326, 330 (2001), Veronia School Dist.47J v. Acton, 515 U.S. 646, 653 (1995); and In re Sealed Case, 310 F.3d at 745.

82. Available at *http://www.fas.org/sgp/crs/intel/m010506.pdf*.

83. *See http://www.loc.gov/crsinfo/whatscrs.html*.

84. *Id.*

85. CRS memo, *supra* n.82 at 15-16; *see also id.* at 27 ("The statutory language in FISA and the legislative history of the bill that became FISA . . . reflect the Congress's stated intention to circumscribe any claim of inherent Presidential authority to conduct electronic surveillance, as defined by the Act, to collect foreign intelligence information, so that FISA would be the exclusive mechanism for the conduct of such electronic surveillance").

86. *Id.* at 43.

87. "[I]t appears unlikely that a court would hold that Congress had expressly or impliedly authorized the NSA electronic surveillance operations here under discussion . . . ." *Id.* at 44.

88. *Id.* at 44.

89. 542 U.S. 507, 520.

90. *See* the posts by George Washington University Professor Orin S. Kerr regarding this topic on "The Volokh Conspiracy" blog, *available at http://www.Volokh.com* (last accessed Jan. 6, 2005).

91. 50 U.S.C. § 1805(f).

92. *See especially* CRS memo, *supra* n.82 at 3-7.

93. 310 Fd. 3d at 720-721, 746.

94. *See* CRS memo, *supra* n.82 at 17, discussing the effect of the repeal of former 18 U.S.C. § 2511(3).

95. 343 U.S. 579, 630, 637-638 (1952) (Jackson, J. concurring). *See* CRS memo at 14 (the NSA program "*may* fall under the third tier of Justice Jackson's formula . . . ." (italics added).

96. 343 U.S. 579, 630, 637-638 (1952) (Jackson, J. concurring).

97. 542 U.S. 507, 535 (plurality opinion of O'Connor, J.). Justice Souter joined in the result based on his interpretation of the AUMF. 542 U.S. 507, 239 (Souter, J., concurring in part, dissenting in part, and concurring in the judgment). On the due process issue, he stated: "I do not adopt the plurality's resolution of constitutional issues that I would not reach. It is not that I could disagree with the plurality's determination (given the plurality's view of the Force Resolution) that someone in Hamdi's position is entitled at a minimum to notice of the Government's claimed factual basis for holding him, and to a fair chance to rebut it before a neutral decision maker . . . ." 542 U.S. at 553.

98. *See especially* CRS memo, *supra* n.82 at 8, 27-232.

99. Surveillance could have been conducted pursuant to the original 50 U.S.C. § 1805(f) for 24 hours before the Attorney General sought approval from the FISA Court. *See* Pub. L. 95-511, Title I, § 105(f). That time-period was extended to 72 hours on December 28, 2001. *See* Pub. L. 107-108, § 314(a)(2)(B).

100. *Id.* at 42-43.

101. 50 U.S.C. §§ 1801(f)(1)–(4).

102. 50 U.S.C. § 1801(i).

103. 50 U.S.C. § 1801(l).

104. James Risen and Eric Lichtblau, *supra* n.1; James Risen and Eric Lichtblau, *supra* n.10.

105. S. Rep. No. 95-604(I), at 65, *reprinted at* 1978 U.S.C.C.A.N. 3904, 3937 (1978).

106. *Id.* at 35 n.39, *reprinted at* 1978 U.S.C.C.A.N. at 3937 n.39 (1978), *citing* Vol. III of the Church Committee report, at 733, *et seq.*, and Vol. II at 58-60, 108, and 308-311.

107. *See* Church Committee report, Vol. II, 308-09 ("The Committee recommends first that the NSA monitor only foreign communications. . . . To the extent that other agencies are required to obtain a warrant before monitoring the communications of Americans, NSA should be required to obtain a warrant.").

The Economic Valuation of Trade Secret Assets

By R. Mark Halligan and Richard F. Weyand

The economic valuation of trade secret assets has perplexed the intellectual property bar for years. The economic and legal issues are seemingly inextricably intertwined. We present here a method for valuation of trade secret assets that decouples the economic and legal issues, rendering the problem tractable.

Several accepted methods exist for the valuation of a property. Depreciated cost, replacement cost, fair market value, and net present value of future cash flows are all proper measures in specific circumstances.

For intellectual property, however, depreciated cost is not appropriate. The direct acquisition cost of intellectual property may be insignificant, as when the intellectual property results from a flash of insight. However, that same insight may result from the sudden emergence of an idea after years of study in the field and years of experimentation in the laboratory. Which, then, is the true cost, the negligible cost of a moment's insight or the sum total cost of the education and experience of a lifetime?

Similarly, replacement cost is problematic. How does one replace a flash of insight? By what means can one predict the machinery of invention? For patents, trademarks, and copyrights, injunctive relief is true replacement, that is, the restoration of the exclusive use of the intellectual property. But trade secrets, once lost in the public domain, are lost forever. The bell cannot be unrung. How then can a replacement cost even be conceptualized, much less determined?

As for fair market value, there may be no marketplace for the intellectual property in question. An advance in the method of manufacturing a proprietary product, a unique corporate organizational structure or compensation plan, negative know-how, that is, knowledge about what doesn't work—none of these intellectual properties has a marketplace from which a fair market value may be obtained.

What we are left with, then, for trade secrets is the ***net present value of future cash flows***. This is a particularly appropriate measure for trade secrets because the very essence of a trade secret anticipates future cash flows. A trade secret is any information not generally known in the trade, which the owner has made appropriate efforts to keep secret and which confers a ***competitive advantage*** from being kept secret. The net present value of future cash flows resulting from that competitive advantage is an appropriate method for placing a dollar amount on the current value of a trade secret asset.

THE NET PRESENT VALUE OF FUTURE CASH FLOWS METHOD

Net present value of a future cash flow requires an evaluation of three factors:

1. The total amount of future cash flow,
2. The discounted basis of that future cash flow as a present value, and
3. The probability of the future cash flow occurring.

If values can be assigned to these three factors, then the economic value of a trade secret can be calculated by multiplying these three factors together.

The total amount of the future cash flow is the total amount of income over time that will be derived from keeping the information secret as compared to the expected income over time if the information was in the public domain. This is analogous to the valuation of patents, where the economic value of the patent is the value of the exclusive use of the invention as compared to the situation in which the invention is available for use by all.

It may be legitimately asked whether there isn't a broader altruistic value in discovering new knowledge for the use of all, to the benefit of everyone. There is such value, but it is not economic value, that is, it is not a value on which a price can be put, such as in the sale or license of a technology. No one will pay for the use of public domain knowledge, and so the fair market value of such knowledge is zero.

Note that there may be more than one legitimate possessor of a trade secret in the marketplace. Calculation of the net present value of trade secrets is much easier if the trade secret is an invention not known at all in the trade. Since in practice it is impossible to determine whether one's competitors already have legitimate possession of the same information and are also holding it as a trade secret, the simple calculation of value comparing the situations of exclusive possession to public domain exposure is appropriate.

R. Mark Halligan is a principal at Welsh & Katz, Ltd. Richard F. Weyand is president of The Trade Secret Office, Inc.

THE ECONOMIC VALUATION OF TRADE SECRET ASSETS

By R. Mark Halligan and Richard F. Weyand

The economic valuation of trade secret assets has perplexed the intellectual property bar for years. The economic and legal issues are seemingly inextricably intertwined. We present here a method for valuation of trade secret assets that decouples the economic and legal issues, rendering the problem tractable.

Several accepted methods exist for the valuation of a property. Depreciated cost, replacement cost, fair market value, and net present value of future cash flows are all proper measures in specific circumstances.

For intellectual property, however, depreciated cost is not appropriate. The direct acquisition cost of intellectual property may be insignificant, as when the intellectual property results from a flash of insight. However, that same insight may result from the sudden emergence of an idea after years of study in the field and years of experimentation in the laboratory. Which, then, is the true cost, the negligible cost of a moment's insight or the sum total cost of the education and experience of a lifetime?

Similarly, replacement cost is problematic. How does one replace a flash of insight? By what means can one predict the machinery of invention? For patents, trademarks, and copyrights, injunctive relief is true replacement, that is, the restoration of the exclusive use of the intellectual property. But trade secrets, once lost in the public domain, are lost forever. The bell cannot be unrung. How then can a replacement cost even be conceptualized, much less determined?

As for fair market value, there may be no marketplace for the intellectual property in question. An advance in the method of manufacturing a proprietary product, a unique corporate organizational structure or compensation plan, negative know-how, that is, knowledge about what doesn't work—none of these intellectual properties has a marketplace from which a fair market value may be obtained.

What we are left with, then, for trade secrets is the ***net present value of future cash flows***. This is a particularly appropriate measure for trade secrets because the very essence of a trade secret anticipates future cash flows. A trade secret is any information not generally known in the trade, which the owner has made appropriate efforts to keep secret and which confers a ***competitive advantage*** from being kept secret. The net present value of future cash flows resulting from that competitive advantage is an appropriate method for placing a dollar amount on the current value of a trade secret asset.

THE NET PRESENT VALUE OF FUTURE CASH FLOWS METHOD

Net present value of a future cash flow requires an evaluation of three factors:

1. The total amount of future cash flow,
2. The discounted basis of that future cash flow as a present value, and
3. The probability of the future cash flow occurring.

If values can be assigned to these three factors, then the economic value of a trade secret can be calculated by multiplying these three factors together.

The total amount of the future cash flow is the total amount of income over time that will be derived from keeping the information secret as compared to the expected income over time if the information was in the public domain. This is analogous to the valuation of patents, where the economic value of the patent is the value of the exclusive use of the invention as compared to the situation in which the invention is available for use by all.

It may be legitimately asked whether there isn't a broader altruistic value in discovering new knowledge for the use of all, to the benefit of everyone. There is such value, but it is not economic value, that is, it is not a value on which a price can be put, such as in the sale or license of a technology. No one will pay for the use of public domain knowledge, and so the fair market value of such knowledge is zero.

Note that there may be more than one legitimate possessor of a trade secret in the marketplace. Calculation of the net present value of trade secrets is much easier if the trade secret is an invention not known at all in the trade. Since in practice it is impossible to determine whether one's competitors already have legitimate possession of the same information and are also holding it as a trade secret, the simple calculation of value comparing the situations of exclusive possession to public domain exposure is appropriate.

R. Mark Halligan is a principal at Welsh & Katz, Ltd. Richard F. Weyand is president ofThe Trade Secret Office, Inc.

Misappropriation creates another possessor of the trade secret without the trade secret owner's authorization or consent. Under these circumstances, the damages evaluation compares the pre-misappropriation market to the post-misappropriation market, and the plaintiff can obtain its lost profits and disgorgement of the misappropriator's ill-gotten gains to the extent not already taken into consideration in calculating the trade secret owner's losses. If other competitors remain ignorant of the information, the damages so calculated will be some portion of the total value calculated when comparing the situations of exclusive possession to public domain exposure.

The second factor in the trade secret valuation model, the discounted basis of a future cash flow, is that percentage of the future cash flow that must be invested now as principal to realize the calculated future cash flows over the expected life cycle of the trade secret. This is a traditional accounting method for the calculation of the present value of a future income stream.

The last factor in the trade secret valuation model is the probability of future cash flows derived from the trade secret asset, which can be calculated by evaluating and determining the probability of prevailing in a civil lawsuit to defend the trade secret asset. This has been the critical barrier preventing the economic valuation of trade secret assets because it has been widely held that the probability of prevailing in a future litigation cannot be calculated. The authors disagree with this general consensus.

A trade secret can be validated only in litigation. Until there is a judgment entered in a civil lawsuit that the plaintiff possesses a trade secret, there is no legal trade secret status. In contrast, there is a presumption of validity when patent, copyright, and trademark certificates are issued by the United States government. An official certificate defines the specific intellectual property right that exists.

TRADE SECRETS IN LITIGATION

Trade secrets, however, remain inchoate and subject to the vagaries of the litigation process. The burden of proof is on the trade secret owner to show the existence of a trade secret as plaintiff in a misappropriation lawsuit. The plaintiff cannot rely on presumptions flowing from a prior *ex parte* examination by the federal government.

There are four proofs required to prevail on an assertion of trade secret protected status in court:

1. Existence. The information must qualify as a trade secret asset.
2. Ownership. The plaintiff must be able to prove ownership of the information.
3. Access. The plaintiff must prove the defendant had access to the information, that is, that the defendant did not independently re-invent the trade secret.
4. Notice. There must be actual, implied or constructive notice of the trade secret status of the information prior to the misappropriation.

Failure of any of these four essential proofs puts the trade secret assets at risk.

The identification of the *res* is critical to proving existence in trade secret litigation. What is "it" that is alleged to be a trade secret? Any information, technical or non-technical, can qualify under the modern definition of a trade secret if the information is not generally known in the trade, there have been appropriate steps taken to protect the secrecy of the information, and there is an actual competitive advantage derived from the secrecy of the information.

These inquiries inevitably require a careful consideration of the following six factors derived from the original definition of a trade secret in the United States in § 757 of the First Restatement of Torts:

1. The extent to which the information is known by outsiders;
2. The extent to which the information is known by insiders;
3. The measures taken to guard the secrecy of the information;
4. The value of the information to the information owner's current operations and the value if obtained by competitors;
5. The amount of time, effort, and money expended to obtain the information; and
6. The ease or difficulty of reverse engineering the information.

All six factors need not be present. However, the six factors will be considered by the trier of fact, and the probability of the existence or non-existence of a trade secret can only be determined after all the six factors have been evaluated and considered.[1]

In litigation, the defendant will dispute all six factors and further argue (1) that the information is generally known in the trade, (2) that it was not reasonably protected, and (3) that it confers no competitive advantage. Plaintiff need not prevail on all six factors, but the plaintiff ***must prevail*** on the three essential elements of the modern definition of a trade secret outlined earlier. Failure of proof on any one of these essential elements will invalidate the existence of a trade secret.

With regard to the first prong of the modern definition, not generally known in the trade, experience in trade secret misappropriation cases has shown that an "everyone knows it" defense does not prevail absent evidentiary substantiation. The defendant must come forward with evidence from industry publications or present evidence from persons skilled in the art to convince the trier of fact that the information is generally known and used by the other competitors in the marketplace.

The second prong of the modern definition causes the most trouble in real situations. What are appropriate measures to protect the trade secret? The test is defined as relative secrecy, not absolute secrecy. Measures approaching absolute secrecy would prevent exploitation of the trade secret to obtain the resulting economic advantage. Relative secrecy means taking reasonable measures under the circumstances. For example, if a company has already suffered a computer theft of trade secrets, the courts expect a higher level of security in the face of this established and known threat. Courts also apply a sliding-scale analysis to corporations based on size. Larger corporations are expected to have more sophisticated trade secret protection measures than a mom-and-pop business.

The burden of establishing reasonable security measures rests upon the plaintiff. Security measures help the courts define what "it" is that is being protected as a trade secret. For example, if a lockbox is the security measure, then the contents of the lockbox must be the trade secrets. Second, reasonable security measures establish the property interests in the trade secret. Stated differently, why should the courts protect the alleged trade secret if the plaintiff has failed to protect it? The standard of care in the industry comes into play with respect to this prong. Courts will look to the security measures of other competitors in the industry to determine whether the plaintiff has executed the requisite amount of reasonable care

Finally, the third prong of the definition requires competitive advantage, that is to say, an economic advantage. This advantage can take the form of increased revenues or profits for the owner of the information, but it can also take the form of a reduced ability of other firms to compete effectively against the owner of the information. That is, either the trade secret owner's competitive position is enhanced by the possession of the information or the competitors' position is diminished by lack of knowledge of the information. Trade secrets also deter entry of new market entrants who must spend the time, effort, and money, go down all the blind alleys, and engage in all the trial and error necessary to compete against the existing competitors in the market.

The second required proof, ownership, has been implied but has not often been litigated, probably because the word "ownership" is not expressly included in the definition. However, it is critical that the possessor of a trade secret have ownership or be a licensee of the owner. The intellectual property laws in the United States protect the creator with few exceptions (*e.g.*, the work-for-hire doctrine in the copyright statute), and the plaintiff must show ownership of the trade secret. Absent an employee-assignment clause in a valid and enforceable employment contract, the result in litigation may be that a trade secret does in fact exist, but it was created and is owned by the employee. The company may retain no more than a shop right to practice the inventions embodied in the trade secret because it was created with company tools on company time

Access is an important proof to secure the plaintiff's trade secret rights. There is no monopoly right in trade secrets. If the defendant can show that the trade secret was independently developed without access or use of the plaintiff's information, then the defendant has the right to practice the inventions or improvements embodied in the trade secret. Trade secret protection can be extended only to prevent actions by employees or third parties that obtain access to the information in confidence and breach that obligation of confidentiality.

Finally, notice of the trade secret status of the information is necessary. The courts will imply constructive notice in a principal-agency relationship under certain circumstances. With respect to third parties, however, failure to provide notice and to obtain an agreement to maintain the information as confidential ***before*** actual disclosure may result in forfeiture and therefore be fatal to the trade secret claim. This is why nondisclosure agreements (NDAs) and confidential disclosure agreements (CDAs) must be executed before third-party disclosures. Although a writing is not required to establish notice, it is clearly preferred to the conflicting testimony of witnesses in a subsequent court hearing.

Notice can take the form of "confidential and proprietary" labels on sensitive documents, a high-level description of the trade secrets on a trade secret exit interview form, or password-protected access on a computer. The failure to mark a document as confidential is not fatal, however, if it can be independently established that the recipient knew or had reason to know that the information was confidential and that the recipient was not authorized to take and use the information for his own benefit or the benefit of others without the trade secret owner's consent.

It is important to note that this required notice cannot take the lackadaisical form that "everything we do is a trade secret." A failure to differentiate the trade secret information from the public domain information within the company places all information in the same class. Companies have found that, when they claim that "everything" is a trade secret, the courts conclude that "nothing" is a trade secret. There is no substitute for the specific identification and protection of trade secret assets by a company.

Where does all this leave us with regard to the economic valuation of a trade secret? There are two important observations to make at this point.

First, the total value of all the potential trade secret information of a company that has failed to meet the evidentiary criteria outlined above should be set at ***exactly zero***. There is no inherent right to obtain trade secret status in information absent proper stewardship, and, absent such stewardship, the probability of prevailing on the merits in future litigation alleging trade secret status for the information approaches zero.

Second, the valuation of a trade secret is not confined to the value of the information content *per se*. ***The valuation of a trade secret asset is a function of both the content of the trade secret information and the stewardship and protection of the trade secret asset.***

This fundamental principle of trade secret asset valuation presents good news and bad news scenarios to corporations faced with the task of performing an economic valuation of their trade secret assets.

It is certainly bad news to the well-meaning but poorly prepared client, after the misappropriation, on the brink of litigation, that its suit has little chance of success due to poor stewardship. The good news is that the implementation of procedures for the proper stewardship and protection of trade secrets ***before misappropriation*** can both ensure and increase the economic value of those assets.

CASE STUDY

We present the following case study to illustrate these principles. As trade secret cases are by definition very sensitive, this case study is necessarily hypothetical. We have combined certain common issues that we have seen in actual cases in order to construct a likely scenario.

In our example, the owner of a closely held company has contacted you to perform an economic valuation of its trade secret portfolio. You perform an initial investigation and find that:

1. There is no inventory of the alleged trade secrets.
2. There are no employee agreements beyond the statutory fiduciary obligations.
3. There are no contractor or visitor agreements.
4. Alleged trade secret information is not secured in locked file cabinets, and such information is often left out in the open on company desks in unlocked offices.
5. Alleged trade secret information is stored on personal computers on which login protections have not been implemented.
6. Documents containing potential trade secrets are not stamped or labeled confidential or proprietary.
7. There is no secure method for destroying confidential documents.
8. No method is in place to track the time, effort, and money expended in creating and developing the alleged trade secret information.
9. Employee, contractor, and visitor badges are not required.
10. There is no security at the front door.
11. The manufacturing processes are not hidden from public view.
12. Temporary workers are often hired during peak periods and exposed to the alleged trade secrets.
13. There is no policy handbook on trade secrets, and no training in trade secret handling procedures for employees.
14. There are no trade secret exit interviews of departing employees.

You inform the business owner that the valuation of his trade secrets has been performed, at far less expense than he had hoped. That's the good news. The bad news is that the economic value of his trade secret information is exactly zero. While the content may or may not have economic value from not being generally known in the trade, there is little probability that the company can or will prevail in litigation. Why should the courts protect information that the company itself has not protected? The company risks forfeiture of its trade secret rights to anyone exposed to such information who can then legally appropriate them for his or her own benefit.

The owner of the company is appalled by the results of your valuation study, shared in confidence with the client. How can this information, developed over many years at great expense, have an economic value of zero? The answer is clear. There is no inherent right or title to trade secrets absent proper stewardship. There is undoubtedly information that provides an economic advantage, but the company has voluntarily exposed it to the world without restriction, and any trade secret rights in this information are at immediate risk of forfeiture.

The case law is replete with examples of this hypothetical. Many information owners find out when it is too late that the courts will not protect their information assets as trade secrets because the company has taken inadequate measures to protect such information, or a forfeiture of any trade secret rights in such information has occurred. Information is either a trade secret or not a trade secret. Absent a patent, if the information is not a trade secret, then the information can be legally appropriated and used by others for their own benefit or the benefit of others.

The unfortunate result in *Omega* v. *Chroma*[2] is illustrative. Several former Omega employees formed a new company using Omega proprietary technology. Omega sued the defendants for trade secret misappropriation. The trial court found that the information at issue was protectible as a trade secret, but Omega lost because the court found that Omega had failed to take reasonable steps to protect the information. Omega's appeal to the Vermont Supreme Court centered on the trial court's finding that the substantial amounts of information acquired and used by the former employees were found to qualify as "trade secrets" by the trial court thereby entitling Omega to judgment as a matter of law. However, the Vermont Supreme Court rejected this argument and affirmed the trial court. The failure of Omega to take adequate steps to protect its trade secret assets resulted in a forfeiture of these trade secret assets and a finding that the former Omega employees owed no duty of confidentiality to Omega.

PROTECTING BEFORE MISAPPROPRIATION

However, in many circumstances, it is *not* too late to change the economic value of the assets because there has been no misappropriation yet. To protect the economic value of trade secret assets, the following basic steps must be implemented.

- An inventory of the potential trade secret assets should be conducted immediately. In practical terms, this will involve the preparation of a list of trade secrets with documentation of the dates of creation, places of storage, places of use, and other key information necessary for the maintenance of these assets on an on-going basis.
- Employee, contractor, and visitor agreements should be implemented. Careful attention should be paid to both confidentiality and ownership issues, with contractual assignment clauses being implemented where necessary.
- With respect to paper documents and tangible items, procedures for locked file cabinets or other security measures should be implemented.
- Electronic security procedures should be implemented, including, at a minimum, the implementation of login protections on personal computers.
- Access to information should be on a need-to-know basis. Sign-out/sign-in procedures should be used. Confidential documents should be marked "confidential." Super-confidential documents should be marked "super-confidential," and access should be severely restricted.
- Locked bins should be used to discard confidential documents, and an outside company performing onsite document destruction should maintain the bins.
- Accounting procedures should be implemented to track the time, effort, and money expended on the creation and development of trade secret assets.
- All persons should wear prominently displayed badges while on the premises. A visitor sign-in/sign-out badge system should be implemented.
- Manufacturing processes should be restricted from public view.
- The company handbook should devote an entire section to trade secrets. There should be ongoing employee education on the importance of identifying and documenting the existence of trade secret assets, with employee economic incentives for complying with this policy.
- The company should implement a strict procedure for trade secret exit interviews.

Once the information is secure and ownership, access, and notice issues are under control, we have changed the zero probability of being able to defend the trade secret information and its resulting future cash flows to a near certainty that protected status will be granted. At this point, the evaluation of the economic value of the ***content*** of the trade secret information can be performed in the same manner as currently practiced for patents. Finally, the current economic value of the trade secret information can be calculated by multiplying the three factors described earlier.

MANAGING TRADE SECRETS

We conclude with a short discussion of an important further distinction between trade secrets and the other intellectual properties—patents, copyrights, and trademarks—and the implications of this distinction. The actual number of patents, copyrights, and trademarks owned by most companies is small, numerable, and changes slowly over time.

In contrast, even small companies may have a very large number of trade secrets. These trade secrets are not so well bounded and defined as patents, copyrights, and trademarks, and so they tend to blend into each other, forming an interlocking mesh of information that does not easily divide into separate, countable, and distinct trade secrets. Finally, trade secrets are created and destroyed rapidly in an information economy, making the management of trade secrets a dynamic process.

The dynamic trade secret environment of firms in our modern economy has led many to conclude that it is simply too difficult, even overwhelming, to address all of these rapidly changing assets on any organized basis. However, the marketplace is demanding an accounting system to track and value intangible information assets. We therefore must provide appropriate solutions for the management of trade secrets by our clients.

The computer revolution that is driving the dynamic trade secret environment holds the promise of a solution as well. Automated systems for the inventorying, tracking, and life-cycle management of trade secrets are becoming available, and we must incorporate these solutions in providing quality intellectual property legal services. As these systems come into wider use, the relative standard of appropriate care for trade secret information will come to include such systems as a necessary element of proper stewardship.

NOTES

1. *See* Learning Curve Toys, Inc. v. Playwood Toys, Inc., 342 F.2d. 714 (7th Cir. 2003).
2. Omega v. Chroma, 174 Vt. 10, 800 A.2d 1064 (2002).

JOURNAL OF INTERNET LAW
Distribution Center
7201 McKinney Circle
Frederick, MD 21704
www.aspenpublishers.com